IMPACT EDUCATION NORTH WEST
I'M POSITIVE ABOUT CHANGE TODAY

www.impactnorthwest.org.uk • office@impactnorthwest.org.uk
0151 328 1561 • 07568060086

Data Privacy Policy

January 2022

Date approved:	January 2022
Approved by:	Head of Centre
Frequency of review:	Biennially
Next review due:	January 2024

INTRODUCTION

This Data Privacy Policy provides you with important information about what, how, where, why and when the Company collects, processes, stores and shares Personal Data belonging to our employees, workers and third parties e.g. customers, suppliers (**Third Party Data**).
The focus of this policy is on:

- the Company's duties and responsibilities in respect of the Personal Data of our employees and workers (**Staff**); and
- the duties and responsibilities our Staff have when they Process the Personal Data of our Staff, and/or when they Process Third Party Data.

DATA PRIVACY: THE BASICS

The Company Processes your Personal Data in accordance with data protection law. This includes the Data Protection Act 2018, and the retained UK law version of the General Data Protection Regulation (EU 2016/679) (**Data Protection Legislation**). It also includes legal principles established via case law. Where applicable, we will also follow any relevant Code(s) of Practice published by the Information Commissioner.

In legal terms, under the Data Protection Legislation, this process of collecting and processing Personal Data means that the Company is referred to as a Controller (**Controller**).

Any external person or organisation that Processes Personal Data on our behalf and on our instructions (e.g. a payroll provider or insurance company) is referred to a Data Processor (**Data Processor**).

Any activity that involves the use of Personal Data is referred to as Processing (**Processing** / **Process** / **Processes**). It includes:

- Obtaining, recording or holding Personal Data (e.g. asking Staff to complete personnel forms);
- Carrying out any operation or set of operations on Personal Data such as organising, amending, retrieving, using, disclosing, erasing or destroying it (e.g. recording relevant information on a personnel file, or maintaining pay records); and
- Transmitting or transferring Personal Data to third parties (e.g. transferring payroll data to HMRC).

IMPACT EDUCATION NORTH WEST
I'M POSITIVE ABOUT CHANGE TODAY
www.impactnorthwest.org.uk • office@impactnorthwest.org.uk
0151 328 1561 • 07568060086

What do we mean by 'Personal Data'?

Types of Personal Data			Not Personal Data
Personal Data	**Special Category Data**	**Criminal Offence Data**	
Name Address Telephone number Date of birth Salary Bank account details National Insurance number Sex and/or gender identity Qualifications and/or professional memberships Employee identification or payroll number Online identifiers (e.g. your IP address) Marital status and dependants Next of kin, emergency contact and death benefit nominee(s) information Bank account details, payroll records and tax status information Annual leave records Information about your entitlement to pension and other benefits Evidence of your right to work in the UK/immigration status (e.g. your passport or driving license) Employment and personnel records (e.g. your contract, work history, promotions or job changes, absences, attendance, and training) Performance and appraisal information	Racial or ethnic origin Political opinions Religious or similar beliefs Trade union membership Physical or mental health conditions (e.g. sick notes, medical reports) Sexual life Sexual orientation Biometric data (e.g. facial imaging or fingerprint data) Genetic data (e.g. DNA or RNA analysis)	Criminal offences and convictions (e.g. DBS checks) Criminal allegations (proven or unproven) Criminal charges, prosecutions or proceedings Investigations Measures imposed on an individual through the criminal justice system or civil measures that may result in a criminal offence if not followed	Truly anonymous data Data that has had your identity permanently removed (e.g. statistical information about the gender breakdown of our workforce from which you cannot be identified)

IMPACT EDUCATION NORTH WEST
I'M POSITIVE ABOUT CHANGE TODAY
www.impactnorthwest.org.uk • office@impactnorthwest.org.uk
0151 328 1561 • 07568060086

Disciplinary and grievance information Photographs Accident book, first aid records, injury at work and third-party accident information Opinions about you (e.g. references provided during recruitment)			

Personal Data (**Personal Data**) is any information that 'relates to' an identified or identifiable individual. It includes information relating to an individual, from which we can identify the individual directly or indirectly (e.g. because it includes their name) (**Data Subject**).
It also includes information relating to an individual, from which they cannot be directly identified, if they can be identified from that information when it is used in combination with other information we hold about that individual.

Personal Data can include information relating to an individual that has been 'pseudonymised', meaning that any information that directly or indirectly identifies the individual (e.g. their name) is removed and replaced with one or more artificial identifiers or pseudonyms (e.g. an employee reference number).

However, truly anonymous data, or data that has had any identifying information permanently removed from it, does not count as Personal Data.

When considering whether information 'relates to' an individual for the purposes of Data Protection Legislation, we take into account a range of factors, including the content of the information, the purpose or purposes for which we are Processing it, and the likely impact or effect of that Processing on the individual Data Subject.

Personal Data includes two subcategories of personal information that attract enhanced legal protection under Data Protection Legislation:

- **Special Category Data**: Personal Data which is particularly sensitive; and
- **Criminal Offence Data**: Personal Data relating to criminal activity, criminal allegations, criminal charges, criminal investigations and proceedings, criminal convictions and offences (See below: CRIMINAL OFFENCE DATA).

The following table gives a non-exhaustive list of examples of what is included and excluded from these definitions:

Criminal Offence Data

In addition to the definition of Criminal Offence Data above, Personal Data will also come within the scope of this category if it concerns;

- Unproven allegations;

www.impactnorthwest.org.uk • office@impactnorthwest.org.uk
0151 328 1561 • 07568060086

- Information relating to the absence of convictions; and
- Personal Data relating to alleged and actual victims, along with witnesses of crime.

Where individuals are subject to security measures which relate to penalties, conditions or restrictions placed on them as part of the criminal justice system, or civil measures which may lead to a criminal penalty if not followed, these will also be treated as Criminal Offence Data.
Where appropriate and legally permitted, the Company collect Criminal Offence Data as part of the recruitment process (e.g. when we conduct a standard or enhanced DBS criminal record check). We may also be notified from time to time of Criminal Offence Data in the course of employment (e.g. if an employee is suspected to have committed a crime, or if an employee reports a criminal conviction to us).

We will only use any Criminal Conviction Data we hold in the following ways:

- To determine whether an individual's criminal record (i.e. the results of a standard or enhanced DBS check) impacts upon their suitability to be offered employment;
- To consider whether any criminal charges, prosecutions or convictions (including cautions) that occur during employment impacts upon the individual's continued suitability for their role, and/or must be reported by us to our insurers, or to regulatory authorities. Company will only collect and Process Criminal Offence Data if it is appropriate given the nature of the individual's role, and where we a lawful basis to do so. This will usually be where Processing is necessary to carry out our obligations.

For the avoidance of doubt, this Data Protection Policy is our appropriate policy document for the purposes of Part 4, Schedule 1 of the Data Protection Act 2018.

RIGHTS, DUTIES AND RESPONSIBILITIES WHEN HANDLING PERSONAL DATA

Your rights in respect of your own Personal Data

Each Data Subject has legal rights designed to protect the privacy of their Personal Data. You are a Data Subject with regard to your own Personal Data. Upon starting employment, and from time to time thereafter, you will be provided with a Data Privacy Statement (**DPS**), which explains how the Company Processes your Personal Data, and provides you with personalised information about your own rights as a Data Subject.

Your duties and responsibilities when handling the Personal Data of third parties

To the extent that you are involved in the Processing of the Personal Data of any third parties (including other members of Staff), you will have legal duties and responsibilities that you must comply with.
This means that you must Process the Personal Data of third parties in compliance with:

- this Data Privacy Policy;
- the law governing data privacy, including the Data Protection Legislation and any relevant Code(s) of Practice issued by the Information Commissioner.

IMPACT EDUCATION NORTH WEST
I'M POSITIVE ABOUT CHANGE TODAY
www.impactnorthwest.org.uk • office@impactnorthwest.org.uk
0151 328 1561 • 07568060086

For further information, see "Our commitment to complying with data protection procedures" below.
You are reminded that any breach of our data privacy policies or procedures, may result in disciplinary action. In certain circumstances, if the Data Protection Legislation is not followed, it may also lead to criminal charges being brought against you personally. As a Controller of Personal Data, we will be obliged to assist the Information Commissioner in any lawful investigations arising out of the Processing of Personal Data.
Staff members whose role involves regular Processing of Personal Data, or might reasonably bring them into contact with Personal Data, will receive training on our data privacy policies and procedures as part of their induction, and this training will be refreshed at regular intervals thereafter (see "Staff Training" below).

Data privacy: our collective responsibility

The Company takes its legal obligations and responsibilities regarding data privacy very seriously and recognises that it is our collectively responsibility to ensure that good data privacy principles are incorporated by design into our systems. This collective responsibility for data privacy means that the Company expect:

- All of our Staff to treat any Personal Data they may come into contact with sensitively and in accordance with our data privacy policies and procedures, and the Data Protection Legislation. This is true regardless of whether or not it is part of their usual role to handle Personal Data.
- Expect all of our Staff to familiarise themselves with our data privacy policies and procedures and to request further information and/or training from their line manager if they are unsure of their duties and obligations under those policies and procedures;
- Expect our managers and directors to lead by example and reinforce the message that the Company takes data privacy seriously; and
- Expect all of our Staff to report any data privacy issues they encounter to the leadership team.

OUR COMMITMENT TO COMPLYING WITH THE PRINCIPLES

Personal Data must be Processed in compliance with the Principles) relating to the Processing of Personal Data (**Principles**) in accordance with Data Protection Legislation.

As the Controller, the Company is responsible for, and must be able to demonstrate compliance with, the DPP (**Accountability principle**).

The Principles require Personal Data to be:

	Principles	**Details**
1.	Processed lawfully, fairly and in a transparent manner (**Lawfulness, Fairness and Transparency**)	Personal Data must be Processed on the basis of one or more of lawful conditions specified in the Data Protection Legislation.

IMPACT EDUCATION NORTH WEST
I'M POSITIVE ABOUT CHANGE TODAY
www.impactnorthwest.org.uk • office@impactnorthwest.org.uk
0151 328 1561 • 07568060086

2.	Collected only for specified, explicit and legitimate Purposes and not further Processed in a manner that is incompatible with those purposes (unless an exception applies) (**Purpose Limitation**)	If we collect Personal Data directly from Data Subjects, we will inform the Data Subject about:
		• The Purpose(s) for which we intend to Process their Personal data; • The third parties (if any) with which we will share, or to which we will disclose, their Personal Data; and • Their rights as a Data Subject (e.g. to access and rectify their Personal Data). Personal Data must not be Processed in any manner incompatible with those original purposes (unless an exception applies).
3.	Adequate, relevant and limited to what is necessary in relation to the Purposes for which it is Processed (**Data Minimisation**)	We will only collect Personal Data to the extent that it is required for the specific Purpose notified to the Data Subject.
4.	Accurate and where necessary kept up to date and with every reasonable step taken to ensure that inaccurate Personal Data is erased or rectified without delay (**Accuracy**).	We will ensure that Personal Data we hold is accurate and kept up to date. We will check the accuracy of any Personal Data at the point of collection and at regular intervals afterwards. You are required to keep us informed of any changes to your Personal Data so that we can keep our records accurate We will take all reasonable steps to, without delay, erase or rectify inaccurate or out-of-date Personal Data.

IMPACT EDUCATION NORTH WEST
I'M POSITIVE ABOUT CHANGE TODAY
www.impactnorthwest.org.uk • office@impactnorthwest.org.uk
0151 328 1561 • 07568060086

5.	Not kept in a form that permits identification of a Data Subject for longer than is necessary for the Purposes for which the data is Processed (**Storage Limitation**).	We follow current data retention guidelines and have procedures for the deletion and destruction of data in accordance with those guidelines.
6.	Processed in a manner that ensures its security, using appropriate technical and organisational measures to protect against unauthorised or unlawful Processing and against accidental loss, destruction or damage (**Integrity and Confidentiality**).	We take appropriate security measures against unlawful or unauthorised Processing of Personal Data, and against the accidental loss of, or damage to, personal data. We have put in place procedures and technologies to maintain the security of all Personal Data from the point of collection to the point of destruction. Personal data will only be transferred to a Data Processor if they agree to comply with those procedures and policies, or if they also put in place adequate security measures.

In addition to the Principles outlined above, in compliance with the Data Protection Legislation, the Company will ensure that Personal Data is:

- Made available to the Data Subject on request and that Data Subjects are allowed to exercise certain rights in relation to their Personal Data. We will Process all Personal Data in line with Data Subjects' rights, in particular their right to:

  - Request access to any Personal Data held about them;
  - Prevent the Processing of their Personal Data for direct-marketing Purposes;
  - Ask to have inaccurate Personal Data amended; and
  - Prevent Processing that is likely to cause damage or distress to the Data Subject or anyone else.

- Not transferred to people/organisations situated in countries without adequate protection. We may only transfer any Personal Data we hold to a country outside the UK provided that one of the following conditions applies:

IMPACT EDUCATION NORTH WEST
I'M POSITIVE ABOUT CHANGE TODAY
www.impactnorthwest.org.uk • office@impactnorthwest.org.uk
0151 328 1561 • 07568060086

- The country ensures an adequate level of protection for the Data Subjects' rights and freedoms;
- The Data Subject has given consent;
- The transfer is necessary for a lawful condition set out in the Data Protection Legislation (e.g. for the performance of a contract between us and the Data Subject, or to protect the vital interests of the Data Subject);
- The transfer is legally required on important public interest grounds or for the establishment, exercise or defence of legal claims; or
- The transfer is authorised by the Information Commissioner where we have adduced adequate safeguards with respect to the protection of the Data Subjects' privacy, their fundamental rights and freedoms, and the exercise of their rights.

CONDITIONS FOR PROCESSING

To be Processed lawfully, Personal Data must be Processed on the basis of one or more of the Conditions specified in the Data Protection Legislation (**Condition(s)**). The most common Conditions we rely on to Process Personal Data are:

CONDITIONS FOR PROCESSING WHICH WE COMMONLY RELY ON	
Personal Data	**Special Category Personal Data & Criminal Offence Data**
• The Data Subject has given his consent to the Processing for one or more specific Purposes • Processing is necessary for entering or performing a contract with the Data Subject • Processing is necessary for compliance with a legal obligation to which the Controller is subject • Processing is necessary to protect the vital interests of the Data Subject Processing is necessary for the Purposes of legitimate interests pursued by the data controller or by a third party	• The Data Subject has given explicit consent to the processing for one or more specific Purposes • Processing is necessary for the Purpose of carrying out the obligations and exercising specific rights of the Controller or of the Data Subject under employment, social security or social protection law • Processing is necessary for a substantial public interest • Processing is necessary to protect the vital interests of the Data Subject or of another natural person, where the Data Subject is physically or legally incapable of giving consent • Processing is necessary for the establishment, exercise or defence of legal claims

www.impactnorthwest.org.uk • office@impactnorthwest.org.uk
0151 328 1561 • 07568060086

	• Processing is necessary for the Purposes of preventive or occupational medicine, for the assessment of the working capacity of the employee, medical diagnosis, the provision of health or social care or treatment or the management of health or social care systems and services

In addition, where we Process any Special Category Data or Criminal Offence Data, we must also be able to show that the Processing meets a condition under Schedule 1, Data Protection Act 2018. This includes were Processing necessary for the purposes of performing or exercising obligations or rights that are imposed or conferred by law in connection with employment, social security or social protection. We may also process these types of Personal Data for a substantial public interest such as preventing or detecting unlawful acts, equalities monitoring or supporting individuals with medical conditions and disabilities.

Purposes

Personal Data must only be collected or Processed for specified, explicit and legitimate Purposes. The Company will establish and record the Condition for Processing each time Processing of Personal Data occurs.
Staff are forbidden from Processing Personal Data for Purposes which go beyond or are incompatible with the original Purposes specified to the Data Subject in the transparency information provided to them (see "Transparency: notifying Data Subjects" below). In the event that you are proposing to use Personal Data in a way which appears not to be consisting with the purpose for which it was collected, please seek advice from the Leadership Team.

Consent

Consent (**Consent**) is one of the many Conditions upon which the Processing of Personal Data can be based. However, in lots of circumstances the Company will rely on other Conditions to process Personal Data instead of relying on Consent. For example, the Company does not routinely rely on Consent as a Condition to justify the Processing of the Personal Data of our Staff. This is explained further in your personal Data Privacy Statement.

When engaging with third parties the Company may rely on Consent as the condition for processing Personal Data. Where we do, the law requires Consent to be in a specific form and to meet specified requirements for it to be deemed valid.
Key points to note about relying on Consent as a Condition for Processing:

- Consent requires affirmative action; silence, pre-ticked boxes or inactivity should not be considered to be consent;
- Consent must be kept separate from other terms and conditions, so that it is clear and unambiguous;
- Use clear and plain language when explaining and requesting consent;

IMPACT EDUCATION NORTH WEST
I'M POSITIVE ABOUT CHANGE TODAY
www.impactnorthwest.org.uk • office@impactnorthwest.org.uk
0151 328 1561 • 07568060086

- Consent must be specific and informed, meaning it should be clear to the Data Subject what it is they are consenting to and how and why their Personal Data will be Processed;
- The Data Subject must be free to refuse to give their Consent to the Processing without fear of negative consequences;
- If Consent is relied upon, the Data Subject must be easily able to withdraw their Consent to Processing at any time and withdrawal must be promptly honoured;
- Consent should be refreshed if Personal Data will be Processed for a different and incompatible Purpose to that disclosed when the Data Subject first consented;
- Consent should not be relied upon as a Condition for Processing where there is an imbalance of power between the Company and the Data Subject; and
- Records should be kept of any Consent received (what consent was given, when and how it was obtained).

WHAT RIGHTS DO DATA SUBJECTS HAVE?

Data Subjects have certain rights when it comes to how we handle their Personal Data. Some of these rights are dependent on the nature and Purposes of the Processing. In summary, these include rights to:

- Withdraw consent to Processing at any time where we have relied on consent to conduct the Processing (see above "Consent");
- Receive certain information about our Processing activities (see "Transparency: notifying Data Subjects" below);
- Request access to the Personal Data that we hold on them (see "Subject Access Requests" below); • Prevent our use of their Personal Data for direct marketing Purposes;
- Ask us to erase Personal Data if it is no longer necessary in relation to the Purposes for which it was collected or Processed, or to rectify inaccurate data or to complete incomplete data;
- Restrict Processing in specific circumstances;
- Challenge Processing which has been justified on the basis of our legitimate interests or in the public interest;
- Request a copy of an agreement under which Personal Data is transferred outside of the UK;
- Prevent Processing that is likely to cause damage or distress to them or anyone else;
- Be notified of any Personal Data Breach which is likely to result in a high risk to their rights and freedoms;
- Make a complaint to the Information Commissioner; and
- In limited circumstances, receive or ask for their Personal Data to be transferred to a third party in a structured, commonly used and machine-readable format.

Staff who receive a written request from a Data Subject who wishes to exercise any of these privacy rights (for example, requesting the rectification or deletion of their Personal Data) should forward it to the Leadership Team immediately.

IMPACT EDUCATION NORTH WEST
I'M POSITIVE ABOUT CHANGE TODAY
www.impactnorthwest.org.uk • office@impactnorthwest.org.uk
0151 328 1561 • 07568060086

Subject Access Requests

Data Subjects may make a formal request for details of the Personal Data we hold about them (**Subject Access Request**). Such requests can be made orally or in writing. The Data Protection Legislation requires us to deal with Subject Access Requests within strict time limits (usually within one month of receipt). Therefore, Staff who receive a written request for access to Personal Data (whether or not the request specifies that it is a Subject Access Request) should forward it to the Leadership Team immediately.

When receiving telephone enquiries, we will only disclose Personal Data we hold on our systems if we check the caller's identity to make sure that information is only given to a person who is entitled to it. If we are not sure about the caller's identity, or if their identity cannot be checked, we will ask that the caller put their request in writing.

TRANSPARENCY: NOTIFYING DATA SUBJECTS

Data Protection Legislation requires Controllers to provide clear, detailed and specific information to Data Subjects about the Processing of their Personal Data. Such information must be provided through appropriate privacy notices. These notices should include:

- The identity of the Controller;
- The contact details of our Leadership Team
- The Purpose of, nature and legal basis for Processing;
- Details of transfers to third countries and the safeguards in place;
- Data retention periods;
- The Data Subject's rights with regard to their Personal Data (e.g. the right to rectification or deletion, the right to withdraw Consent and the right to be forgotten); and
- Details of any automated decision-making, any profiling, and how they will be used to make decisions.

The Data Protection Legislation (and the accompanying guidance) is very specific about the language used in any privacy notices. Therefore, to ensure compliance, the Leadership Team must be involved in the drafting of any privacy notices. In the event that the Company is to engage in new Processing activity or to engage a new third party service provider a workflow must be included to ensure that the privacy information provided to Data Subjects has been updated and/or remains reflective of what we do.

Your Personal Data Privacy Statement

Your personal Data Privacy Statement provides you with the required information in relation to our Processing of your Personal Data. From time to time, your personal Data Privacy Statement will be updated to reflect any changes to the Processing of your Personal Data.

IMPACT EDUCATION NORTH WEST
I'M POSITIVE ABOUT CHANGE TODAY
www.impactnorthwest.org.uk • office@impactnorthwest.org.uk
0151 328 1561 • 07568060086

Third Party Data: timing of privacy notices

The point at which we must provide the Data Subject with a privacy notice depends upon how the Personal Data is collected by the Company:

- **Personal Data is collected directly from the Data Subject**: A notice containing all of the required information must be provided to the Data Subject at the point when the Personal Data is collected;
- **Personal Data is collected indirectly (e.g. from a third party)**: The Data Subject must be provided with a notice containing all of the required information as soon as possible (but in any event within one month) after we receive the Personal Data. Before Processing Personal Data that has been obtained indirectly, you must also check that the Personal Data was collected by the third party in accordance with the Data Protection Legislation, and on a basis which contemplates our proposed Processing of that Personal Data.

PURPOSE LIMITATION

Personal Data must be collected only for specified, explicit and legitimate Purposes (**Purpose(s)**) and must not be further Processed in any manner incompatible with those Purposes. This means that we cannot use Personal Data for new, different or incompatible Purposes from that disclosed when it was first obtained, unless we have informed the Data Subject of the new Purposes, and (if this is the Condition relied upon to Process their Personal Data) they have given their Consent. To ensure compliance with this Purpose limitation requirement:

- The Company will establish and record the Purposes for Processing each time Personal Data is collected;
- Staff who are responsible for collecting or Processing Personal Data must ensure on each occasion that the Purposes for doing so are compatible than the original specified Purposes. If the Purposes are incompatible, the Data Subject must be notified of the new Purposes before their Personal Data is Processed for the new Purposes.

You are reminded that Processing Personal Data for Purposes incompatible with the Purposes for which the Personal Data was obtained, is considered a serious breach of this Data Privacy Policy and may result in disciplinary action.

DATA MINIMISATION

Personal Data must be adequate, relevant and limited to what is necessary in relation to the Purposes for which it is Processed. This means that you:

- May only collect or Process Personal Data when performing your job duties requires it;
- Cannot Process Personal Data for any reason unrelated to your job duties;
- Must not collect excessive Personal Data, which is not relevant for the specified Purposes;

IMPACT EDUCATION NORTH WEST
I'M POSITIVE ABOUT CHANGE TODAY
www.impactnorthwest.org.uk • office@impactnorthwest.org.uk
0151 328 1561 • 07568060086

- Must ensure that when any Personal Data is no longer needed for the specified Purposes, it is deleted or anonymised in accordance with [the Company's Data Retention Policy OR current data retention guidelines].

DATA ACCURACY

Personal Data must be accurate and, where necessary, kept up to date. It must be corrected or deleted without delay when inaccurate. To the extent that your job requires you to collect or Process Personal Data, this means that you:

- Must ensure that the Personal Data we Process is accurate, complete, kept up to date and relevant to the Purpose(s) for which we collected it;
- Must check the accuracy of any Personal Data at the point of collection and at regular intervals afterwards; and
- Must take all reasonable steps to destroy or amend inaccurate or out-of-date Personal Data.

STORAGE LIMITATION

Personal Data must not be kept in an identifiable form for longer than is necessary for the Purpose(s) for which the data is Processed. The Company (and to the extent that your duties involve the Processing of Personal Data, you) must not keep Personal Data in a form which permits the identification of the Data Subject for longer than needed for the legitimate business Purpose(s) for which we originally collected it.
The Company will follow current data retention guidelines (outlined below) which are] designed to ensure Personal Data is deleted after a reasonable time, unless a law requires such Personal Data to be kept for a minimum time.

TYPE OF EMPLOYMENT RECORD	RETENTION PERIOD
Job applications and interview records of unsuccessful candidates	6 months after notifying unsuccessful candidates
Personnel and training records	7 years after termination
Working time records	7 years
Annual leave records	7 years
Wage, payroll and PAYE records	7 years
Maternity records	7 years after the end of the tax year in which the maternity pay period ends
Current bank details	Until final salary payment is made
Records of advances and loans made to employees	7 years after repayment
Death benefit nomination/revocation forms	7 years after payment of benefit or termination of employment
Any reportable accident, death or injury in connection with work	4 years after incident

IMPACT EDUCATION NORTH WEST
I'M POSITIVE ABOUT CHANGE TODAY
www.impactnorthwest.org.uk • office@impactnorthwest.org.uk
0151 328 1561 • 07568060086

Disclosure and Barring Service (DBS) checks and other disclosures of criminal records	Deleted after recruitment process unless assessed as relevant to on-going employment relationship (then deleted once the conviction is spent unless it is an excluded profession).
Right to work in the UK checks	3 years after termination
Disclosure and Barring Service (DBS) checks and other disclosures of criminal records	Deleted 6 months after recruitment process unless assessed as relevant to the on-going employment relationship (then deleted once any convictions are spent, unless it is an excluded profession)

The Company (and to the extent that your duties involve the Processing of Personal Data, you) will:

- Take all reasonable steps to destroy or erase from our systems all Personal Data that we no longer require in accordance with the Company's [Data Retention Policy OR current guidelines on Data Retention (outlined above)]; and
- Ensure Data Subjects are informed in any applicable privacy notice of the period(s) for which their Personal Data is stored.

DATA SECURITY

The Company will take appropriate security measures against unlawful or unauthorised Processing of Personal Data, and against the accidental loss of, or damage to, Personal Data. We have procedures and technologies in place, which are designed to maintain the security of Personal Data from the point of collection to the point of destruction. In summary, this means that the Company and our Staff must ensure that:

- Only people who are authorised to use the Personal Data can access it;
- Steps are taken to ensure that people who are authorised to access Personal Data are not accessing or Processing Personal Data for reasons which are unrelated to their job role;
- Steps are taken to verify the identity of a Data Subject before discussing their Personal Data with them;
- Personal Data is stored on the Company's central computer system instead of individual PCs, laptops, tablet devices, mobile telephones etc;
- Computers and laptops are not left unattended without locking their screens via password controls to prevent unauthorised access;
- Personal Data is not carried outside of the building, save on permitted storage devices which are encrypted and password protected or when it is legally necessary to do so such as for statutory safeguarding meetings.

IMPACT EDUCATION NORTH WEST
I'M POSITIVE ABOUT CHANGE TODAY
www.impactnorthwest.org.uk • office@impactnorthwest.org.uk
0151 328 1561 • 07568060086

- Personal Data Breaches, or circumstances which might reasonably lead to a Personal Data Breach, are promptly reported; and
- Our security procedures [e.g. e.g. door entry controls, use of secure locking cupboards/filing cabinets, shredding procedures] are followed.

You are reminded that any breach of our data security procedures is considered a serious breach of this Data Privacy Policy and may result in disciplinary action. In certain circumstances, breaches may also lead to criminal charges being brought against you personally.

Staff Training

As part of our commitment to data security staff whose role involves regular Processing of Personal Data , or which might reasonably bring them into contact with Personal Data will receive training on our data privacy policies and procedures as part of their induction and this will be refreshed at regular intervals thereafter.

DATA PRIVACY IMPACT ASSESSMENTS

In certain circumstances, the Company is legally required to perform a Data Protection Impact Assessment (**DPIA**) in order to identify and minimise the data privacy risks of a project. A DPIA is required if we plan to:

- Use systematic and extensive profiling with significant effects;
- Process Special Category Personal Data or Criminal Conviction Data on a large scale;
- Systematically monitor publicly accessible places on a large scale;
- Use innovative technology (in combination with any of the criteria from the European guidelines);
- Use profiling or Special Category Personal Data to decide on access to services;
- Profile individuals on a large scale;
- Process biometric data (in combination with any of the criteria from the European guidelines);
- Process genetic data (in combination with any of the criteria from the European guidelines);
- Match data or combine datasets from different sources;
- Collect personal data from a source other than the individual without providing them with a privacy notice ('invisible processing') (in combination with any of the criteria from the European guidelines);
- Track individuals' location or behaviour (in combination with any of the criteria from the European guidelines);
- Profile children or target marketing or online services at them; or
- Process data that might endanger the individual's physical health or safety in the event of a security breach.

It is the responsibility of all Staff to promptly notify the Leadership Team if they consider there is a risk that any of the above circumstances applies, or will apply.

IMPACT EDUCATION NORTH WEST
I'M POSITIVE ABOUT CHANGE TODAY
www.impactnorthwest.org.uk • office@impactnorthwest.org.uk
0151 328 1561 • 07568060086

It is also good practice to do a DPIA for any other major project that requires the Processing of Personal Data and Staff can speak to the Leadership Team for further guidance on how to complete a DPIA.

Any DPIA must:

- Describe the nature, scope, context and Purposes of the Processing;
- Assess necessity, proportionality and compliance measures;
- Identify and assess risks to individuals; and
- Identify any additional measures to mitigate those risks.

MANDATORY DATA BREACH REPORTING

Under the Data Protection Legislation, the Company has certain obligation to mandatorily report Personal Data Breaches. A Personal Data Breach (**Personal Data Breach**) is a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, Personal Data transmitted, stored or otherwise Processed.

There are two levels of mandatory reporting obligation, which depend upon the level of risk arising from the Personal Data Breach:

Mandatory Reporting Obligation	Details
Report to Information Commissioner must be made ASAP (at latest within 72 hours of becoming aware of the Personal Data Breach).	If the Personal Data Breach is likely to result in **a risk** to Data Subject's rights and freedoms. Examples: • Report: – the loss of customer details which leaves individual Data Subjects open to identity theft; – a ransomware attack which results in all personal data being encrypted and no back-ups are available;
	• Do not report: – internal loss of a staff telephone list; – loss of a securely encrypted mobile device, provided the encryption key remains within our secure possession and this is not the sole copy of the Personal Data.

IMPACT EDUCATION NORTH WEST
I'M POSITIVE ABOUT CHANGE TODAY
www.impactnorthwest.org.uk • office@impactnorthwest.org.uk
0151 328 1561 • 07568060086

Notify Data Subject "without undue delay" and "as soon as reasonably feasible".	If a Personal Data Breach poses a **high risk** to a Data Subject, then it must be directly reported to them as well as the Information Commissioner unless an exception applies. High-risk situations are likely to include the potential of people suffering significant detrimental effect – for example, discrimination, damage to reputation or financial loss. Examples of high-risk Personal Data Breaches: • A cyber-attack leads to Personal Data being exfiltrated from our server; • We suffer a ransomware attack, which results in all Personal Data being encrypted. No back-ups are available, and the data cannot be restored; and • We suffer a cyber-attack and usernames, passwords and purchase history are published online by the attacker. There are some limited exceptions to the mandatory requirement to report a Personal Data Breach to the Data Subject.

Failure to make the relevant mandatory Personal Data Breach report may lead to a financial sanction against the Company.

It is the responsibility of all Staff to **immediately** report any Personal Data Breach which comes to their attention (whether it involves you personally, or any other member of Staff, whether subordinate or senior to you), or any circumstances which might reasonably be interpreted as a Personal Data Breach, or which could lead to a Personal Data Breach to the Leadership Team.

If you are involved in a suspected Personal Data Breach you will be required to fully assist those investigating it in a timely manner and to provide as much information as possible to identify if a breach has occurred and the extent of any potential risk to those individuals involved.

DATA PROTECTION OFFICER

The Company has appointed a Data Protection Officer, who has overall responsibility for the Company's policies and procedures relating to data privacy. The Data Protection Officer should be your first point of contact in the following situations:

- If you have any concerns, or require clarification, about your or the Company's obligations regarding data privacy;
- If you have any feedback or suggestions about how the Company can improve its data privacy and/or data security procedures;
- If you receive a request from a Data Subject seeking to:

www.impactnorthwest.org.uk • office@impactnorthwest.org.uk
0151 328 1561 • 07568060086

- Access their Personal Data (see "Subject Access Requests" above); or
- Exercise any of their other rights as a Data Subject (see "What rights do Data Subjects have?" above), such as to withdraw their Consent to Processing;

- If you become aware of any member of Staff:
  - Abusing their role to access Personal Data for non-permitted reasons;
  - Processing Personal Data in a manner which is inconsistent with this Data Privacy Policy;
  - [Committing a breach of our Data Security Policy.

- If you, or any other member of Staff (whether subordinate or senior to you), are involved in a Personal Data Breach, or circumstances which might reasonably be interpreted as a Personal Data Breach, or which could lead to a Personal Data Breach (see "Mandatory Data Breach Reporting" above).

Our Data Protection Officer is: Jo Smith. Contact details are: 07568 060 086, jo@impactnorthwest.org.uk
Impact North West Ltd, Unit 1, Tower House, Tower Road, Birkenhead, Wirral, CH41 1FF.